Profitability in Peace: Protecting Nuclear ICS Vulnerabilities

Article By: Lindsey Warner, Consultant, Deloitte & Touche, LLP

Introduction:

ICS is a growing security industry that continues to evolve from cyber-attacks to causing physical damage with a click of a button. From anywhere in the world ICSs can be targeted and damaged in a matter of seconds by exploiting vulnerabilities. While threats and risks are not new, the scale in which an ICS outage can disrupt top targeted industries is a continuous learning curve. ICS attacks are significantly increasing, thus the business surrounding ICS challenges evolving technologies. ICS cyber-attacks are alarmingly rising due to a demand to profit from real world risk. These attacks are defining a new movement in securing ICS from outdated technologies into a new automated digital tool, which also changes the scope of incoming malicious activity. While the probability of modernization of Nuclear ICSs mitigates exposure to global and national vulnerabilities, new system operational challenges and clandestine operations, the long-term profitability in funding on a large scale today allows for a better protected tomorrow.

Nuclear ICS on a Global Front

The emergence of ICS as a key weakness in the global cyberwarfare race has intensified over the years to form one of the most dangerous frontline damaging attacks. The longstanding Israeli-Iran tête-à-tête, most notably the cyber-attack on Iran's Natanz plant and Israeli water treatment plant attacks, are another reminder of how quickly grids can be shut down. These strongly echo the Stuxnet stunt that demonstrated the full scale of how dangerous cyber-attacks can be on ICSs. These attacks can result in physical damage as well as business interruption which affects a globalized economy. Critical infrastructure is a major target for terrorist groups as well as government entities as it's hard to differentiate between espionage and malfunction. As nuclear plants are one of the most vulnerable infrastructures to protect, mostly due to outdated systems being converted to OT, malicious groups are constantly targeting these plants on a global front. Nuclear vulnerabilities extend further than just damaging property or potential loss of life, it can trigger a lack of credibility in deterrence or even provoke military response. Weapons systems are critically underdeveloped in most reported cyber vulnerabilities, leading to miscalculation and misunderstanding between nation states and their allies. Thirty countries have operational nuclear power, and approximately fifty are under construction. Nuclear vulnerabilities on a global front are a top priority for securing ICS, but especially for the United States as modernization becomes a primary focus.

Nuclear ICS and the United States

The United States is leading the way in providing and mitigating Nuclear ICS vulnerabilities by thoroughly understanding how cyber-attacks are at the forefront of game-changing risks. While all countries are vulnerable, the US is a hot target for malicious intent with 60 commercially operating nuclear power plants to protect. Cyber threats are becoming more sophisticated every day and staying ahead of the curve is increasingly difficult when the risk is associated with

nuclear command, control, and communications. The most recent Log4j vulnerability shows the immense pressure malicious attackers can inflict remotely on targeted devices. The US response to ICS cyber-attacks has heavily relied on the private sector to modernize cyber defenses to meet the threat of ransomware. The most recent published statement from the White House details next steps as a nation by stating:

"The [Biden] Administration has announced specific efforts to encourage resilience, including voluntary cyber performance goals, classified threat briefings for critical infrastructure executives and the Industrial Control Systems Cybersecurity Initiative. And, the Administration has stepped up to lead international efforts to fight ransomware. International partnership is key since transnational criminal organizations are often the perpetrators of ransomware crimes, leveraging global infrastructure and money laundering networks to carry out their attacks."

The US is working towards peaceful solutions in fighting cyber-attacks as the overall risks outweighs any type of credible reward. As the US navigates the next frontier in malicious attacks, resiliency will extend to the modernization of OT as Nuclear systems transition to a digital scope.

Nuclear ICS and Modernization Challenges

The US is underway in replacing decades old nuclear systems over the next twenty years, with additional capability upgrades. The Congressional Budget Office (CBO) estimated that the US will spend a total of $634 billion over the next 10 years to modernize the nuclear arsenal. Modernization the US is focusing on includes Modernized Strategic Delivery Systems, Refurbished Nuclear Warheads, Modernized Production Complex and Command and Control Systems. Nuclear exploitations with Programmable Login Controllers (PLCs) have been on the radar for over a decade but remain exposed due to slow upgraded systems as well. While these modernization tactics are a necessary expense, competing pressure and sustaining complex life extension for the supply chain are critical challenges nuclear ICSs will face. Focusing on modernization prevents the potential shut down, blown centrifuges or data collection that old technologies have a harder time being protected from. The readiness and response of US nuclear arms control is a direct correlation between the changing movement to cyber conflicts in place of visible military action. As nuclear weapons and ICSs are overhauled for the first time in forty years, reliance on digital tools that feature new automation and machine learning will challenge how governments entangle themselves within each other. Digital openness extends the opportunities for further exploitation and cyber espionage related targets.

Nuclear ICS and Clandestine Operations

Nuclear cybersecurity incidents have a history of being underreported due to nontraditional attacks occurring by unknown perpetrators. Cyber-attacks change the scope of attacks by making it difficult to disrupt, freeze, and sometimes physically destroy ICS through technology. Cyber espionage has increasingly been used to collect information under the radar with malicious purposes in mind. SolarWinds is a recent example of how spying malware can go undetected for a lengthy period while inflicting damage in the private and government sectors. Spying capabilities on a digital front pose a new threat to ICSs as the intention is to silently collect a

mass amount of data, which can later become weaponized information. Securing ICS environments, especially nuclear industries in an ever-connected world are critical to mitigate economic gain through industrial espionage. Formerly, physically isolating ICS environments made cyber-attacks and espionage more difficult, but as modernization moves full steam ahead, these attacks will increase with serious ramifications.

Profitability in Peace

As nation states covertly infiltrate for data collection and potential malicious intent, the significant damage spills into global economies. Stealing intellectual property, technology innovation and trade secrets are just some of the top economic cash grabs that can cause immeasurable devastation. The U.S. economy has estimated about $600 billion of annual costs occurring from cyber espionage. The economic impact of cyber-attacks, especially to ICSs are a significant enough threat that focusing funds to preemptive measures results in a lesser payout on a global scale. Nuclear ICSs peaceful international relations is exceptionally important to maintain as any instability can cause drastic long-term affects. Reduction in cyber violence is profitable to countries and thus a responsibility to maintain on a large scale. ICS attacks are significantly increasing, therefore the business surrounding ICSs will remain a major focal point as new technologies emerge.

Conclusion

Protecting Nuclear ICSs vulnerabilities in a changing globalized world is a profitable long-term solution. As economic espionage plays a large-scale role in securing the cyber industry, the demand from malicious actors will always be right around the corner. By analyzing past and current cyber infiltrations, nation states can better protect and stay ahead of the curve. Understanding the top targeted industries and countries is a key to allotting the funding and personnel to the right scope. Staying on track with modernization and continuing the efforts as digital tools go online will allow for cyber-attacks to be thwarted. Today's weaknesses in Nuclear ICS networks are tomorrow's old technology that can be utilized to build the next generation of secured systems.